## **SIEMENS**

Data sheet 6XV1850-2GH20

product description

Patch cable, preferred length, preassembled with two RJ45 connectors (10/100MB)

Industrial Ethernet TP Cord RJ45/RJ45, TP cord pre-assembled with 2 RJ45 plug, length 2 m.



suitability for use	Easy connection of terminal devices to the IE FC cabling system			
cable designation	LI 02YSCY 2x2x0,15/0,98 PIMF ICCS GN			
wire length	2 m			
electrical data				
number of electrical connections	2			
attenuation factor per length				
• at 10 MHz / maximum	0.09 dB/m			
• at 100 MHz / maximum	0.285 dB/m			
• at 300 MHz / maximum	0.495 dB/m			
• at 600 MHz / maximum	0.75 dB/m			
impedance				
• at 1 MHz 100 MHz	100 Ω			
• at 10 MHz 600 MHz	100 Ω			
relative symmetrical tolerance				
• of the characteristic impedance at 1 MHz 100 MHz	15 %			
• of the characteristic impedance at 10 MHz 600 MHz	6 %			
transfer impedance per length / at 10 MHz	10 mΩ/m			
loop resistance per length / maximum	300 mΩ/m			
insulation resistance coefficient	150 GΩ·m			
operating voltage				
RMS value	80 V			
mechanical data				
number of electrical cores	4			
design of the shield	Overlapped aluminum-clad foil, sheathed in a braided screen of tin-plated copper wires			
core diameter				
<ul> <li>of AWG26 insulated conductor</li> </ul>	0.48 mm			
outer diameter				
of inner conductor	0.48 mm			
of the wire insulation	0.98 mm			
width / of cable sheath	5.8 mm			
symmetrical tolerance of width / of cable sheath	0.2 mm			
thickness / of cable sheath	3.7 mm			
symmetrical tolerance of thickness / of cable sheath	0.2 mm			
material				
<ul> <li>of the wire insulation</li> </ul>	polyethylene (PE)			
of cable sheath	PVC			
color				
<ul> <li>of the insulation of data wires</li> </ul>	white/blue, white/orange			

bending radius  • with single bend riminimum permissible  • with single bend riminimum permissible  • with multiple bends riminimum permissible  • with multiple bends riminimum permissible  • with grant temporature  • curring peration  • curring peration  • curring peration  • curring peration  • curring resistance  • curring resistance  • curring resistance  • curring resistance  • confidence and control of the behavior  • curring resistance  • confidence and control of the behavior  • confidence of suitability  • confidence of suitabil	of cable sheath	green			
with single bend / minimum permisable		3.000			
with multiple bends / minimum permissible     weight per length     32 kg/km     samblent conditions     amblent temperature	-	24 mm			
weight per length subtent conditions  ambient temperature  - during storage - during steadance -					
ambient temperature  - during poperation  - during storage  - during transport  - duri	·				
ambient temperature  • during storage • during storage • during stransport • during st	<u> </u>				
during spreadon     during stronge     during stronge     during stronge     during stronge     during strangort     du 0. +70 °C     during installation     figure resistant according to IEC 60332-2-1  free behavior     figure resistant according to IEC 60332-2-1  chomical resistance     to mineral oil     to grease     product for strong product functions, product components / general     product feature     haldgoen free     No     salicon-free     yes     salicon-free     No     yes     salicon-free     No     yes     salicon-free     No     was posifications, approvals  ULLETE, listing / 300 V Rating     ULLETE, styler, 600 V Rating     Certificate of suitability     EAC approval     Yes     salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     Salicon-free     No     No     Salicon-free     No     No     No     No     No     No					
during stranger     during transport     during installation     during i	·	-40 +70 °C			
during transport     during installation     during installation     fire behavior     firm behavior     firm resistant according to IEC 60932-2-1     chemical resistance     to mineral oil		-40 +70 °C			
during installation     fire behavior     fire behavior     for onineral oil					
fire behavior Chemical resistance 1 on inherat oil 2 of greace 1 to miherat oil 3 oil resistant according to IEC 60931-2-1 (4 h / 70°C) Conditional resistance 1 to greace Protection class IP Protection clas					
chemical resistance  • to mineral oil • to grease protection class IP  product features • halogen-free • halogen-free • halogen-free • halogen-free • halogen-free • halogen-free • salacion-free • per sandards, specifications, approvals  ULFET Listing' 300 V Rating  ULFET Listing' 300 V Rating  ULFET Listing' 300 V Rating  Ves • EAC approval • UL approval • LU approval • LU approval • LO approval • LO approval • LO best Norske Verifas (DNV) • Det Norske Verifas (DNV) • Det Norske Verifas (DNV) • Det Norske Verifas (DNV) • Period marine classification society (RV) • Loyds Register of Shipping (LRS) • No • Period marine dustriance budy (GL) • Loyds Register of Shipping (LRS) • No • Poisk Register Station (PRS) • No • Poisk Register Station (PRS) • No • Poisk Register Station (PRS) • No • Poisk Register Station guide for cables and connectors • to web basic: Selection guide for cables and connectors • to web page: selection and IT As Selection Tool • to website: Image database • to		flame resistant according to IEC 60332-2-1			
	chemical resistance	Ĭ			
e to grease product fontures, product functions, product components / general product features	• to mineral oil	oil resistant according to IEC 60811-2-1 (4 h / 70°C)			
product features product functions, product components / general product feature	• to grease				
product feature		IP20			
Silcon-free     Silcon-fr	product features, product functions, product components / gene	eral			
Saladards, specifications, approvals	product feature				
**sillcon-free**  **standards, specifications, approvals  ULFEIL Ising / 300 V Rating  No  ULFEIL style / 600 V Rating  No  certificate of suitability  **EAC approval  **UL approval  **UL approval  **UL approval  **Standard for structured cabling  **American Bureau of Shipping Europe Ltd. (ABS)  **American Bureau of Shipping Europe Ltd. (ABS)  **French marine classification society (BV)  **Det Norske Veritias (DNV)  **Det Norske Veritias (DNV)  **Det Norske Veritias (DNV)  **Det Norske Veritias (DNV)  **Polski Rejestr Statkow (PRS)  **Nepon Kaiji Kyokai (NK)  **Polski Rejestr Statkow (PRS)  **reference code  **according to IEC 81346-2  **according to IEC 81346-2.2019  **WGB  **Urther information / internet links*  internet link  **to website: Selection guide for cables and connectors  **to web page: SiePortal  **to website: Industry Online Support  **to website: Industry Online Support  **statistic: CAx-Download-Manager  **to to website: Industry Online Support  **statistic: Ask-Download-Manager  **to to website: Industry Online	•	No			
UL/ETL Isiting / 300 V Rating  UL/ETL style / 800 V Rating  No certificate of suitability  EAC approval  Ves standard for structured cabling  Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  Fernor harrier classification society (BV)  Det Norske Veritas (DNV)  Oemanische Lloyd (GL)  No  Det Norske Veritas (DNV)  Open Kaiji Kyokai (NK)  Polski Register of Shipping (LRS)  No  No  Polski Register of Shipping (LRS)  No  Polski Register of Staltow (PRS)  No  reference code  according to IEC 81346-2  according to IEC 81346-2  wGB  further information / Internet links  internet link  to website: Selection guide for cables and connectors to web page: SiePortal  to website: Selection guide for cables and connectors to web page: SiePortal  to website: Industry Online Support  Scourtly Information  security information  Security information  Security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and onthrousely an and networks against cyber threats, it is necessary to implement – and onthrousely maintain – a holistic, state-of-the-ari industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing nuarthorized access to their plants, systems, machines and networks against cyber threats, it is necessary to implement – and onthrousely maintain – a holistic, state-of-the-ari industrial cybersecurity concept. Siemens' products and solutions on necessary are in propries a security machines and networks against cyber threats, it is necessary are in propries asserting nuarthorized access to their plants, systems, machines and networks against cyber threats, it is necessary are in propries asserting numericance in the internet if and to the exten		Yes			
UL/ETL Isiting / 300 V Rating  UL/ETL style / 800 V Rating  No certificate of suitability  EAC approval  Ves standard for structured cabling  Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  Fernor harrier classification society (BV)  Det Norske Veritas (DNV)  Oemanische Lloyd (GL)  No  Det Norske Veritas (DNV)  Open Kaiji Kyokai (NK)  Polski Register of Shipping (LRS)  No  No  Polski Register of Shipping (LRS)  No  Polski Register of Staltow (PRS)  No  reference code  according to IEC 81346-2  according to IEC 81346-2  wGB  further information / Internet links  internet link  to website: Selection guide for cables and connectors to web page: SiePortal  to website: Selection guide for cables and connectors to web page: SiePortal  to website: Industry Online Support  Scourtly Information  security information  Security information  Security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and onthrousely an and networks against cyber threats, it is necessary to implement – and onthrousely maintain – a holistic, state-of-the-ari industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing nuarthorized access to their plants, systems, machines and networks against cyber threats, it is necessary to implement – and onthrousely maintain – a holistic, state-of-the-ari industrial cybersecurity concept. Siemens' products and solutions on necessary are in propries a security machines and networks against cyber threats, it is necessary are in propries asserting nuarthorized access to their plants, systems, machines and networks against cyber threats, it is necessary are in propries asserting numericance in the internet if and to the exten					
ULETL style / 600 V Rating  certificate of suitability  EAC approval  UL approval  UL approval  Ves  Standard for structured cabling  Cat5  Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  French marine classification society (BV)  Det Norske Veritas (DNV)  Loyds Register of Shipping (LRS)  No  No  Polski Rejest foliation (PRS)  No  Polski Rejest Stattow (PRS)  No  Polski Rejest Stattow (PRS)  No  Polski Rejest Stattow (PRS)  WG  according to IEC 81346-2  according to IEC 81346-22  according to IEC 81346-22-19  WGB  further information / Internet links  internet link  to website: Selection aid TIA Selection Tool  to web page: selection aid TIA Selection Tool  to website: Image database  to website: CAx-Download-Manager  to website: Image database  to website: Image database  to website: CAx-Download-Manager  to website: Image database  to website: CAx-Download-Manager  to website: Image database  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.  In order to protect plants, systems, machines and networks.  In order to protect plants, systems, machines and networks.  In order to protect plants, systems, machines and networks.  In order to protect plants, systems, machines and networks.  In order to protect plants, systems, machines and networks.  In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously martini — a holistic, state-of-the-art industrial cybersecurity concilores are responsible networks regionate in the product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are and and the towns that and the latest product versions are used. Use of product versions that are		No			
certificate of suitability  EAC approval  UL approval  Ves  UL approval  Yes  Standard for structured cabling  Cat5  Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  French marine classification society (BV)  Det Norske Veritias (DNV)  Det Norske Veritias (DNV)  No  Germanische Lolyd (GL)  Lolyds Register of Shipping (LRS)  No  No  Polski Registr Statkow (PRS)  reference code  according to IEC 81346-2  blues between the state of the sta					
• U. approval     • Ves standard for structured cabling  Marine classification association     • American Bureau of Shipping Europe Ltd. (ABS)     • French marine classification society (BV)     • Det Norske Veritas (DNV)     • Det Norske Veritas (DNV)     • Oermanische Lloyd (GL)     • Lloyds Register of Shipping (LRS)     • Nippon Kajii Kyokai (NK)     • Polski Rejestr Statkow (PRS)     • Polski Rejestr Statkow (PRS)     reference code     • according to IEC 81346-2.2019     further information / Internet links     internet link     • to web page: selection guide for cables and connectors     • to web page: selection aid TIA Selection Tool     • to web page: selection aid TIA Selection Tool     • to website: CAx-Download-Manager     • to website: Image database     • to website: Image database     • to website: Industry Orline Support     ** thips://support.industry.siemens.com/cax     ** thips://support.industry.siemens.com/ca	· · · · · · · · · · · · · · · · · · ·				
standard for structured cabling  Marine classification association  • American Bureau of Shipping Europe Ltd. (ABS)  • French marine classification society (BV)  • Det Norske Veritas (DNV)  • No  • No  • Nopon Kaji (Kyokai (NK)  • Polski Rejestr Statkow (PRS)  reference code  • according to IEC 81346-2  • according to IEC 81346-2  • according to IEC 81346-2-2019  **WGB**  **Internet link  • to web page: Selection gluide for cables and connectors  • to web page: Selection gluide for cables and connectors  • to web page: Selection and TIA Selection Tool  • to web page: Selection and TIA Selection Tool  • to website: Manage database  • to website: CAx-Download-Manager  • to website: Industry Online Support  **Intus://www.siemens.com/baltdb  **Intus://www.siemens.com/balt	•	Yes			
Standard for structured cabling  Marine classification association  • American Bureau of Shipping Europe Ltd. (ABS)  • French marine classification society (BV)  • Det Norske Veritas (DNV)  • Det Norske Veritas (DNV)  • Germanische Lloyd (GL)  • Lloyds Register of Shipping (LRS)  • No  • Nippon Kaiji Kyokai (NK)  • Polski Rejest Statkow (PRS)  reference code  • according to IEC 81346-2  • to website: Selection guide for cables and connectors  • to web page: selection aid TIA Selection Tool  • to web page: selection aid TIA Selection Tool  • to website: Image database  • to website: Image database  • to website: Industry Online Support  • to website: Industry Online Support  **Intos://support.industry.siemens.com/silcoud  **Intos://support.industry.siemens.com/pilddb  **Intos://support.industry.s					
Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  French marine classification society (BV)  Pet Norske Veritas (DNV)  Germanische Lloyd (GL)  No  Lloyds Register of Shipping (LRS)  Nippon Kajii Kyokai (NK)  Polski Rejest Vistatkow (PRS)  No  reference code  according to IEC 81346-2  according to IEC 81346-2  according to IEC 81346-22019  WGB  further information / internet links  internet link  No web page: selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to web page: SiePortal  https://swww.siemens.com/cs/ww/en/view/109766358  https://sww.siemens.com/cs/ww/en/view/109766358  https://sww.siemens.com/cs/ww/en/view/109766358  https://sww.siemens.com/cs/ww/en/view/10	· ·	Cat5			
French marine classification society (BV)  Det Norske Veritas (DNV)  Germanische Lloyd (GL)  Lloyds Register of Shipping (LRS)  No  Nippon Kajii Kyokai (NK)  Poliski Rejestr Statkow (PRS)  Reference code  according to IEC 81346-2  according to IEC 81346-2  according to IEC 81346-2  by WG  Further information / Internet links  internet link  to website: Selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to website: Selection aid TIA Selection Tool  to website: Industry Online Support  https://www.siemens.com/cs/ww/en/view/109766358  https://www.siemens.com/  to website: Industry Online Support  Security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems and networks and networks. In order to protect plants, systems and networks and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems and networks against cyber threats, it is necessary to implement—and continuously mantain—a holistic, state-of-lihe-art industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onetworks.					
French marine classification society (BV)  Det Norske Veritas (DNV)  Germanische Lloyd (GL)  Lloyds Register of Shipping (LRS)  No  Nippon Kajii Kyokai (NK)  Poliski Rejestr Statkow (PRS)  Reference code  according to IEC 81346-2  according to IEC 81346-2  according to IEC 81346-2  by WG  Further information / Internet links  internet link  to website: Selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to website: Selection aid TIA Selection Tool  to website: Industry Online Support  https://www.siemens.com/cs/ww/en/view/109766358  https://www.siemens.com/  to website: Industry Online Support  Security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems and networks and networks. In order to protect plants, systems and networks and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems and networks against cyber threats, it is necessary to implement—and continuously mantain—a holistic, state-of-lihe-art industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onetworks.	American Bureau of Shipping Europe Ltd. (ABS)	No			
Det Norske Veritas (DNV) Germanische Lloyd (GL) Lloyds Register of Shipping (LRS) No No Polski Register of Shipping (LRS) No Polski Rejestr Statkow (PRS) No reference code according to IEC 81346-2 according to IEC 81346-2:2019 WG  further information / Internet links internet link  to website: Selection guide for cables and connectors to web page: Selection aid TIA Selection Tool this://swww.siemens.com/tsticloud ttps://swww.siemens.com/ this://swww.siemens.com/ this://swww.siemens.com/ security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial		No			
Germanische Lloyd (GL) Lloyds Register of Shipping (LRS) No Nippon Kaiji Kyokai (NK) Polski Rejestr Statkow (PRS) No reference code according to IEC 81346-2 according to IEC 81346-2 WGB  Further Information / Internet links internet link to website: Selection guide for cables and connectors to web page: selection guide for cables and connectors to web page: selection guide for cables and connectors to web page: selection aid TIA Selection Tool to website: Image database to website: Industry Online Support thtps://www.siemens.com/cakww.siemens.com/bilddb https://sww.siemens.com/cak thtps://sww.siemens.com/cak security information  security information  Siemens provides products and solutions with industrial cybersecurity functions that support industry, siemens and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement—and continuously maintain — a holistic, state-of-the-art industrial cybersecurity concept. Siemen's products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, anachines and networks segmentation) are in industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are avail		No			
Lloyds Register of Shipping (LRS) No Nippon Kaiji Kyokai (NK) Polski Rejestr Statkow (PRS) No  reference code according to IEC 81346-2 according to IEC 81346-2 according to IEC 81346-2:019 WGB  further information / internet links internet link  to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database to website: Image database to website: Image database to website: Industry Online Support thtps://www.siemens.com/cax https://www.siemens.com/cax https://www.siemens.com/cax  Security information  security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks and networks. Such systems, machines and onection is necessary and only when appropriate security measures text such a connection is necessary and only when appropriate security measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybers	,	No			
No Polski Rejestr Statkow (PRS) No reference code		No			
Polski Rejestr Statkow (PRS)  reference code  according to IEC 81346-2  according to IEC 81346-2  according to IEC 81346-2  WG  wGB  further information / internet links  internet link  to website: Selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to web page: SiePortal  to website: Image database  to website: Image database  to website: Industry Online Support  to website: Industry Online Support  security information  All these is necessary and only when appropriate security measures (e.g. firewalls and one necessary and only when appropriate security measures (e.g. firewalls and/or networks segments only are in place. For additional information on the lates the products and solutions undergree security measures that any be implement—a doubtions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary in plement—a net continuously maintain —a holistic, state-of-the-art industrial cybersecurity concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.slemens.com/coherencements that product versions are used. Use of product versions that are the latest product versions are used. Use of product versions that are		No			
reference code  according to IEC 81346-2  according to IEC 81346-2:2019  WGB  further information / internet links  internet link  a to website: Selection guide for cables and connectors  b to web page: selection aid TIA Selection Tool  to web page: SiePortal  to website: Image database  to website: Image database  to website: CAx-Download-Manager  to website: Industry Online Support  to website: Industry Online Support  security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks and solutions constitute oelement of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cs/www.		No			
according to IEC 81346-2:2019      website: Selection guide for cables and connectors         • to website: Selection guide for cables and connectors         • to web page: selection aid TIA Selection Tool         • to web page: selection aid TIA Selection Tool         • to web page: SiePortal         • to website: Image database         • to website: Image database         • to website: Image database         • to website: Industry Online Support         • to website: Ind					
internet link  • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industry Online Support  security information  security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unathorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and my when appropriate security measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	<ul> <li>according to IEC 81346-2</li> </ul>	WG			
internet link  • to website: Selection guide for cables and connectors  • to web page: selection aid TIA Selection Tool  • to web page: SiePortal  • to website: Image database  • to website: CAx-Download-Manager  • to website: Industry Online Support  security information  security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one tworks segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product versions are used. Use of product versions that are	<ul> <li>according to IEC 81346-2:2019</li> </ul>	WGB			
• to website: Selection guide for cables and connectors     • to web page: selection aid TIA Selection Tool     • to web page: SiePortal     • to website: Image database     • to website: Image database     • to website: Industry Online Support      • to website: Industry Onlin	further information / internet links				
to web page: selection aid TIA Selection Tool     to web page: SiePortal     to website: Image database     to website: Image database     to website: CAx-Download-Manager     to website: Industry Online Support      security information  security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	internet link				
• to web page: SiePortal     • to website: Image database     • to website: CAx-Download-Manager     • to website: Industry Online Support      **Security information**  **Security information**  **Security information**  **Security information**  **Security information**  **Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-ard industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product versions are used. Use of product versions that are	• to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358			
to website: Image database     to website: CAx-Download-Manager     to website: Industry Online Support      security information  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product versions are used. Use of product versions that are	<ul> <li>to web page: selection aid TIA Selection Tool</li> </ul>	https://www.siemens.com/tstcloud			
to website: CAx-Download-Manager     to website: Industry Online Support      https://support.industry.siemens.com  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	to web page: SiePortal	https://sieportal.siemens.com/			
• to website: Industry Online Support    Security information	• to website: Image database	https://www.automation.siemens.com/bilddb			
security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	• to website: CAx-Download-Manager	https://www.siemens.com/cax			
Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	• to website: Industry Online Support	https://support.industry.siemens.com			
that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	security information				
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	security information	Siemens provides products and solutions with industrial cybersecurity functions			
threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are	,	that support the secure operation of plants, systems, machines and networks.			
solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are		networks. Such systems, machines and components should only be connected			
network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are					
and that the latest product versions are used. Use of product versions that are		undergo continuous development to make them more secure. Siemens strongly			
customer's exposure to cyber threats. To stay informed about product updates,		customer's exposure to cyber threats. To stay informed about product updates,			
subscribe to the Siemens Industrial Cybersecurity RSS Feed under		subscribe to the Siemens industrial Cybersecurity RSS Feed under			

## Approvals / Certificates

## **General Product Approval**





Manufacturer Declara-tion

Declaration of Conformity

<u>ate</u>





For use in hazardous locations		Test Certificates	Environment	Industrial Commu- nication	
			Special Test Certific-	Confirmation	PROFINET

last modified:

8/8/2024

